



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/692,530

10/24/2003

Kim Cameron

40062.0218US01

9898

Homer Knearl  
Merchant & Gould P.C.  
P.O. Box 2903  
Minneapolis, MN 55402-0903

7590

09/30/2008

EXAMINER

HOANG, DANIEL L

ART UNIT

PAPER NUMBER

2136

MAIL DATE

DELIVERY MODE

09/30/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/692,530	<b>Applicant(s)</b> CAMERON ET AL.	
	<b>Examiner</b> DANIEL L. HOANG	<b>Art Unit</b> 2136	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 02 July 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1,3-16, 18-20 and 22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-16, 18-20, 22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)<br>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)<br>3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____. | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date _____.<br>5) <input type="checkbox"/> Notice of Informal Patent Application<br>6) <input type="checkbox"/> Other: _____. |
|--|---|

## DETAILED ACTION

### CLAIMS PRESENTED

Claims 1, and 3-16, and 18-22 are presented.

### RESPONSE TO ARGUMENTS

Applicant's arguments filed 7/02/08 have been fully considered but they are not persuasive.

Please see 112 rejections section below regarding applicant's amendments and arguments pertaining to said amendments.

### CLAIM REJECTIONS

#### *Claim Rejections - 35 USC § 112*

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 1, 9, and 16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Said claims recite the limitation of "a use policy providing instructions as to how the group identity information may be used". Applicant's specification does not disclose use policies pertaining to group identity information. Paragraph 28 of the specification recites a usage policy describing how information may be used but only pertains to self-identity information, not the claimed group identity information. Appropriate correction is required.

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 1, 9, and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
5. Claim 1 recites generating a group-signed group identity information document comprising a use policy providing instructions as to how the group identity information may be used. Applicant's specification is mute in disclosing a group identity information document comprising a use policy. As discussed above, a usage policy is only described as being part of self-identity information. It is unclear whether applicant intends for the claim to cite generating a self identity information document (which would provide antecedent basis for the use policy) or a group identity information document (which lacks antecedent basis for the use policy). Since interpreting the claim to recite a self identity information document would require amendments to numerous instances in the claim as well as depending claims, claim 1 will be examined without the above cited limitation. Appropriate correction is required.
6. Claims 9 and 16 recite the same limitation and are also similarly rejected.

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, and 3-16, and 18-21, 22 rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna et al., US Patent No. 6,801,998 and further in view of Huitema et al., US Patent No. 7,068,789.

**As per claim 1, Hanna teaches:**

In an initiating system, a method for establishing a new group identity with a group identity information document comprising:

creating group identity information for inclusion in the group identity information document; and

*[see col. 5, lines 29-33] "In response to the receipt of a request for service from the applicant associated with the client 10, the application server 12 determines the identification of the group or groups having the right to perform the requested service."*

generating a self-signed group identity information document comprising the group identity information, at least a first key, and a group identity information document signature signed using a second key associated with the first key in the identity information document.

*[see col. 5, lines 36-49] "The application server 12 generates an encrypted group identification message, which may take a number of forms. For example, as depicted in FIG. 4a, the encrypted group identification message may be formed by encrypting the relevant group id (i.e. the group id for the group having access to the requested service) with an encryption key which permits decryption by the applicable group membership server 16. More particularly, the application server 12 and the group membership server may have a shared or symmetric key and the group id may be encrypted using the shared key. Alternatively, the applicable group membership server 16 may be provided with a public key pair and the group id may be encrypted using the respective group membership server public key."*

sending the group-signed group identity information document to a receiving system to establish the new group identity at the receiving system.

*[see col. 5, lines 62-65] "The client 10, upon receipt of the encrypted group id, forwards the same to the default group membership server 16 or the applicable group membership server 16 specified in the message."*

Hanna is mute in teaching that the group identity being established at the receiving system is a new group identity being established. As for this limitation, examiner relies on the Huitema reference.

In col. 12, lines 1-17, Huitema teaches the process of creating a new group. It would be obvious to one of ordinary skill in the art to combine the teachings of Hanna and Huitema so that not only existing groups can expand by adding new members but also so that new groups may be securely formed. The process taught by Huitema allows any peer the ability to create a new group and set the security attributes for that new group.

**As per claim 3, Hanna teaches:**

The method of claim 2, further comprising: sending a group-signed membership identity information document with the group-signed group identity information document to the receiving system to establish membership of an originator of the membership identity information document in the new group identity established at the receiving system.

*[see col. 5, lines 58-61] "The message transmitted from the application server 12 to the client 10 that includes the encrypted group id may also include an unencrypted identification of the group membership server 16."*

*As has been cited above in the rejection of claim 1, Huitema teaches that the identity being established is a new group identity.*

**As per claim 4, Hanna teaches:**

The method of claim 3 further comprising:

receiving the new group-signed membership identity information document from the originator;

*[see col. 5, lines 66-67] "The group membership server receiving the encrypted group id decrypts the message to obtain the name of the group having the right of access to the requested service."*

detecting whether the group associated with the membership identity information document has been accepted; and

*[see col. 6, lines 2-4] "The group membership server then determines if the applicant is a member of the specified group."*

assigning security protocols to communications from the originator based on the group identity information if the group identity information is accepted.

*[see col. 6, lines 4-6] "If it is determined that the applicant is a member of the group, the group membership server 16 generates a message indicative of membership."*

**As per claim 5, Hanna teaches:**

The method of claim 3, wherein the act of sending comprises: storing the group-signed membership identity information document in an initiating system; retrieving the group-signed membership identity information document; attaching the group-signed membership identity information document to the message; and sending the message to the receiving system.

*[see fig. 3A and 3B]*

**As per claim 6, Hanna teaches:**

The method of claim 3, further comprising: sending to the receiving system a self-signed personal identity information document of the originator of the message to establish at the receiving system identity of the originator in addition to originator's membership in the new group.

*[see rejection of claim 4, wherein if the group membership server determines if the applicant is a member of the specified group. Examiner is interpreting that it is clear that applicant submits some sort of identification information along with encrypted group ID in order for said server to authenticate/validate applicant.]*

**As per claim 7, Hanna teaches:**

The method of claim 6, wherein the acts of sending a self-signed personal identity information document and group-signed membership identity information document comprises:

generating the self-signed personal identity information document;

*[see rejection of claim 6]*

attaching the self-signed personal identity information document to the message;

*[see rejection of claim 6]*

retrieving the group-signed membership identity information document;

*[see rejection of claim 1]*

attaching the group-signed membership identity information document to the message; and

*[see rejection of claim 1]*

sending the message to the receiving system.

*[see rejection of claim 3]*

**As per claim 8, 19, and 20, Hanna teaches:**

The method of claim 6 further comprising:

receiving the group-signed membership identity information document and the self-signed personal identity information document from the originator;

*[see fig. 3A, element 60]*

detecting whether the new group associated with the membership identity information document is accepted and whether the person associated with the personal identity information document is accepted;

*[see fig. 3A, elements 62 and 74]*

assigning first security protocols to communications from the originator if the new group is accepted; and

*[see fig. 3B, element 78]*

assigning second security protocols to communications from the originator if the person is accepted.

*[see fig. 3B, element 80]*

**As per claim 9 and 16, Hanna teaches:**

In a communication system, an apparatus for establishing a new group identity comprising:

a group ID generate module generating a group certificate having at least a public key and a digital signature for the group; and a send module transmitting the group certificate to establish the group identity at a receiving system.

*[see rejection of claim 1, further see col. 6, lines 10-14] "the message may comprise an encrypted certificate signed by the respective group membership server 16 that indicates that the applicant is a member of the specified group. The certificate is signed by the respective group membership server 16 and encrypted using an encryption key that permits decryption by the application server. This encryption key may comprise a shared key or alternatively, the public key of a public key pair maintained by the application server 12."*

A computer storage medium readable by a computing system and encoding a computer program of instructions for executing a computer process for establishing a new group identity in communications between an initiating system and a receiving system, said computer process comprising:



generating at the initiating system a group certificate comprising at least a group public key and a digital signature for the group signed with a group private key associated with group public key;

sending the group certificate to the receiving system to establish the new group identity at the receiving system;

sending a membership certificate to the receiving system to establish the originator as a member of the new group at the receiving system;

generating a personal certificate having at least a public key of the originator and a digital signature for the originator signed by the originator with a private key associated with the public key of the originator; and

sending the personal certificate to establish the personal identity of the originator at the receiving system.

**As per claim 10, Hanna teaches:**

The apparatus of claim 9 further comprising: an attach module attaching a group membership certificate to a message originated by a sender; the send module transmitting the message to the receiving system to establish the sender as a member of the new group at the receiving system.

*[see rejection of claim 9, encrypted certificate]*

**As per claim 11, Hanna teaches:**

The apparatus of claim 10 further comprising:

a membership ID generate module generating a membership certificate having at least a public key of the sender and a digital signature for the new group;

*[see rejection of claim 9]*

a save module, responsive to the membership ID generate module, storing the membership certificate;

*[see fig. 1, application server]*

a retrieve module retrieving the membership certificate from the save module and providing the membership certificate to the attach module.

*[see fig. 1 application server]*

**As per claim 12, Hanna teaches:**

The apparatus of claim 10 further comprising: a receive module at a receiving system receiving the membership certificate; and an accept module at the receiving system detecting whether to accept the membership certificate.

*[see fig. 1, group membership server]*

**As per claim 13, Hanna teaches:**

The apparatus of claim 12 further comprising: an assign module assigning a security identification to communications from the sender based on the new group associated with the membership certificate if the membership certificate is accepted by the accept module.

*[see fig. 3A, elements 62 and 74]*

**As per claim 14, Hanna teaches:**

The apparatus of claim 10 further comprising: a personal ID generate module generating a personal certificate having at least a public key of the sender and a digital signature by the sender; and

*[see fig. 3A, element 68]*

the send module transmitting the personal certificate to establish the sender's identity at the receiving system.

*[see fig. 3A, element 70]*

**As per claim 15 and 22, Hanna teaches:**

The apparatus of claim 12 further comprising:

a personal ID generate module generating a personal certificate having at least a public key of the sender and a digital signature by the sender;

*[see fig. 3A, element 68]*

a receive module at the receiving system receiving the certificates;

*[see fig. 3A, element 60]*

an accept module at the receiving system detecting if the certificates are to be accepted;

*[see fig. 3A, elements 62 and 74]*

an assign module assigning a security protocol to communications from the sender based on a group identity associated with the membership certificate if the membership certificate is accepted by the accept module; and

*[see fig. 3B, element 78]*

the assign module assigning a security protocol to communications from the sender based on personal identity associated with the personal certificate if the personal certificate is accepted by the accept module.

*[see fig. 3B, element 80]*

### **As per claim 16, Hanna teaches:**

A computer storage medium readable by a computing system and encoding a computer program of instructions for executing a computer process for establishing a new group identity in communications between an initiating system and a receiving system, said computer process comprising:  
generating at the initiating system a group certificate comprising at least a group public key and a digital signature for the group signed with a group private key associated with group public key; sending the group certificate to the receiving system to establish the new group identity at the receiving system;  
sending a membership certificate to the receiving system to establish the originator as a member of the new group at the receiving system;

*[see rejection of claim 1, further see col. 6, lines 10-14] "the message may comprise an encrypted certificate signed by the respective group membership server 16 that indicates that the applicant is a member of the specified group. The certificate is signed by the respective group membership server 16 and encrypted using an encryption key that permits decryption by the application server. This encryption key may comprise a shared key or alternatively, the public key of a public key pair maintained by the application server 12."*

generating a personal certificate having at least a public key of the originator and a digital signature for the originator signed by the originator with a private key associated with the public key of the originator;  
and sending the personal certificate to establish the personal identity of the originator at the receiving system.

*[see col. 5, lines 62-65] "The client 10, upon receipt of the encrypted group id, forwards the same to the default group membership server 16 or the applicable group membership server 16 specified in the message."*

**As per claim 18, Hanna teaches:**

The computer readable medium of claim 16 wherein the process further comprises: creating the membership certificate at the initiating system, the membership certificate having at least a public key of the originator and a digital signature signed using the group private key.

*[see rejection of claim 1]*

**CONCLUSION**

2. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

**POINTS OF CONTACT**

\*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to:**

Commissioner for Patents  
P.O. Box 1450

Alexandria, VA 22313-1450

**Hand-delivered responses** should be brought to

Customer Service Window  
Randolph Building  
401 Dulaney Street  
Alexandria, VA 22314

\*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

*Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).*

/Daniel L. Hoang/  
Examiner, Art Unit 2136

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2136